斯洛伐克 Slovakia（MiCA）加密资产服务提供商（CASP）牌照常见问题（FAQ 大全）

Slovakia (MiCA) Crypto-Asset Service Provider (CASP) License – Complete FAQ (Delivery Version)

本文由 **仁港永胜（香港）有限公司** 拟定，并由 **唐上永（唐生，Tang Shangyong）** 业务经理提供专业讲解。

服务商：**仁港永胜（香港）有限公司**｜**Rengangyongsheng (Hong Kong) Limited**

适用对象：拟以斯洛伐克 Slovakia为 MiCA 申请国（Home Member State），申请并运营 CASP（Crypto-Asset Service Provider），并通过 MiCA **护照机制（passporting）**向全欧盟跨境展业的机构。
法律依据：MiCA（Regulation (EU) 2023/1114）统一授权与持续监管框架。
Travel Rule：TFR（Regulation (EU) 2023/1113）加密资产转账随行信息规则。

斯洛伐克主管机关（NCA）：Národná banka Slovenska（**NBS**）对加密资产（Crypto-assets/CASP 授权）已发布官方 FAQ 与申请沟通指引。
申请时限口径：**NBS 25 个工作日完成"完整性检查"；完整后 40 个工作日作出批准/拒绝决定；斯洛伐克不适用简化程序。**

✅ 点击这里可以下载 PDF 文件：斯洛伐克 Slovakia（MiCA）加密资产服务提供商（CASP）牌照申请注册指南
✅ 点击这里可以下载 PDF 文件：关于仁港永胜

注：本文模板、清单、Word/PDF 可编辑电子档，可向仁港永胜唐生有偿索取（用于监管递交与内部落地）。

牌照介绍

1）牌照名称
牌照名称：**MiCA 体系下 Crypto-Asset Service Provider（CASP）授权**（以斯洛伐克为 Home Member State，获批后可依 MiCA 护照机制在欧盟跨境提供获批范围内的加密资产服务）。

2）斯洛伐克监管坐标（最重要入口信息）

- **主管机关（NCA）：NBS（National Bank of Slovakia）**。NBS 已公开说明：在斯洛伐克从事相关加密资产业务需取得主管机关授权，主管机关即 NBS。
- **跨境"规则与一般良好（Rules of General Good）"**：NBS 已发布针对"来自其他成员国的 CASP 在斯洛伐克提供服务"需遵守的一般良好规则文件，用于护照展业合规落地（营销、消费者保护、投诉等常落在此类"本地一般良好规则"框架里）。

3）一句话结论（给老板/投资人）
斯洛伐克 CASP 的关键不在"写材料"，而在于：把 MiCA 的授权材料做成 **NBS 可审查、可补件、可演示（系统证据链）**的交付包，并从 Day-1 把 **TFR/Travel Rule、AML、DORA/ICT、外包治理、客户披露与投诉机制**做成可运行体系。

斯洛伐克 Slovakia MiCA （CASP）牌照常见问题（FAQ）Q1–Q400

A. 牌照定位与监管框架（Q1–Q20）

Q1：MiCA 下的 CASP 是什么？
A：CASP 是在 MiCA 框架下向客户提供加密资产服务的持牌主体。MiCA 采用"**按服务类别授权**"，获批后可在授权范围内欧盟跨境展业。

Q2：斯洛伐克的 CASP 主管机关是谁？
A：斯洛伐克层面由 **NBS**作为主管机关发布 Crypto-assets 专区与 FAQ，并按 MiCA 时限处理授权申请。

Q3：NBS 的审批时限是多久？
A：NBS 口径：收到申请后 **25 个工作日**评估是否"材料齐备/完整"；若完整，NBS 将在收到完整申请后 **40 个工作日**决定批准或拒绝；且**不适用简化授权程序**。

Q4：为什么说"时限不等于总周期"？
A：因为 25/40 工作日通常在"**完整申请**"基础上起算；多数项目耗时在"补件（RFI）往返、系统证据链补强、股东资金来源解释、外包合同整改"等环节。

Q5：MiCA 与 Travel Rule（TFR）是什么关系？
A：MiCA 管"持牌与持续监管"；TFR 管"转账随行信息（Travel Rule）"。做托管、转账、平台、出入金对接时，监管通常要求两者**同步落地**。

Q6：MiCA 获批后能否直接在欧盟 27 国开展业务？
A：原则上可通过**护照通报**在其他成员国提供服务/设分支，但落地国仍可能对营销、消费者保护、语言披露等提出本地化要求（"护照≠无需本地合规补丁"）。

Q7：MiCA 是否涵盖所有"加密相关业务"？
A：不一定。部分业务（例如某些完全去中心化情形、MiCA 明确排除项、以及与证券法/支付法交叉的业务）需要做**边界判定**，并在商业计划书中清晰写明"监管归属与排除依据"。

Q8：ESMA 近期香港是否有对 CASP 营销提出关注？
A：ESMA 曾公开警示部分机构用"受监管身份"误导客户，把受规管与不受规管产品混同宣传；这会直接影响你在披露与营销合规章节的写法与内部审查流程。

Q9：是否必须在申请阶段就确定最终的服务组合？
A：必须至少确定"**首批申请服务清单**"，因为资本、制度、IT、外包、人员胜任力都要逐项对齐服务类别；后续扩项通常属于变更/增项申请范畴。

Q10：斯洛伐克是否有"过渡/存量 VASP 自动转换 CASP"的简化路径？
A：NBS FAQ 明确：**斯洛伐克不适用简化授权程序**；存量机构也需要按 MiCA 路径准备完整材料与证据链。

Q11：MiCA 申请材料有什么"格式化趋势"？
A：MiCA 的申请信息要素与 ESMA/EBA 的配套 RTS/ITS 体系通常体现为"**表格化字段 + 附件编号交叉引用**"，监管期待材料可审计、可追溯、可补件。

Q12：NBS 是否建议申请前先沟通？
A：NBS 提供"申请前准备/沟通"页面，要求以其指定方式提交问卷/附件并与其沟通申请准备。

Q13：申请主体必须是斯洛伐克公司吗？
A：通常需要在斯洛伐克（或欧盟内）具备可监管的设立形态，以斯洛伐克为 Home Member State 申请时，核心是满足"有效管理 + 实质运营 + 可监管可检查"的监管预期。

Q14：集团结构复杂（多层控股）是否会降低通过率？
A：会显著增加审核工作量：UBO 穿透、控制权解释、资金路径、关联交易与利益冲突、外包与集团共享服务的控制权都要解释清楚。

Q15：股东是非欧盟主体可以吗？
A：可行但会提高 SoF/SoW、制裁筛查、税务居民与资金跨境路径的审查强度；建议把"资金来源—入资路径—治理独立性"做成可审计证据链。

Q16：是否能用"买壳/收购"替代新申请？
A：MiCA 下最终仍需要满足持续义务与变更申报；并购路径通常要做"重大持股审查 + 变更通知/批准 + 控制权与外包重评估"。

Q17：是否必须有本地员工？
A：强烈建议至少关键控制职能在本地（或欧盟内）可履职：合规、AML、风险、信息安全、运营负责人；否则很容易被认定为"空壳/无实质"。

Q18：MiCA 是否要求内审职能？
A：监管期待"三道防线"或等效安排：业务一线、合规/风险二线、内审或独立审查三线；小机构可外包内审但必须有独立性与整改闭环证据。

Q19：MiCA 与 DORA 有何关系？
A：DORA 是金融机构 ICT 韧性法规，MiCA CASP 在 ICT 风险、外包第三方、事件管理、测试与业务连续性方面通常需要与 DORA 对齐（监管问答常会交叉提问）。

Q20：最常见的"第一轮被问"是什么？
A：服务边界不清、Substance 证据不足、资本/现金流不可信、外包合同缺审计权与退出条款、Travel Rule 不可运行、日志/权限/密钥证据链不足。

B. 服务范围与申请组合（Q21–Q45）

Q21：MiCA 下 CASP 主要服务类别有哪些？
A：常见包括托管与管理、运营交易平台、兑换（法币/币币）、执行/传递订单、代表客户转移、投顾/组合管理等（以 MiCA 服务目录为准）。

Q22：为什么"先定服务组合"是第一步？
A：因为不同服务对资本、系统安全、客户资产保护、市场监测、冲突管理、人员胜任力的要求差异巨大；服务不清会导致整套材料不可审计。

Q23：新团队更建议从哪些服务组合切入？
A：通常建议从"制度/AML/Travel Rule 驱动、系统压力相对低"的组合先做（例如偏经纪/传递/转移/执行），再扩展到平台/托管等重资产重系统模块。

Q24：交易平台（Trading Platform）为什么最难？
A：因为要同时证明：平台规则、撮合与订单生命周期、市场监测与滥用识别、上币/下币治理、异常处置、数据与日志可取证、客户披露与公平执行。

Q25：托管（Custody）为什么也很难？
A：监管核心在"客户资产隔离 + 密钥控制 + 权限分层 + 可审计对账 + 赔付责任边界 + 灾备与应急"。任何一项薄弱都会导致补件。

Q26：如果只做"币币兑换"会被要求平台级制度吗？
A：如果你是撮合/做市/聚合报价并面向零售客户，监管仍可能要求公平执行、冲突管理、价格形成与异常报价过滤、费用披露、订单留痕等平台式控制。

Q27：OTC 业务如何在 MiCA 下表述？
A：要拆成服务实质：是否属于兑换、执行、传递、转移、托管；并说明报价机制、对手方风险、反欺诈与 AML 场景、录音留痕、争议处理。

Q28：是否可以申请后再上线某些功能？
A：可以"分阶段上线"，但你必须证明：上线前控制已就绪、上线审批流程明确、系统证据链可验证；不能用"未来会做"替代当下能力证明。

Q29：能否用外包系统来满足平台/托管要求？
A：可行，但外包治理会成为监管重点：审计权、监管可访问、数据权属、分包限制、事件通报、退出迁移与替代方案都必须写入合同与治理制度。

Q30：做 staking/收益产品会增加复杂度吗？
A：会显著增加披露、冲突、适当性、风险揭示与资产处置条款复杂度；还可能触发与证券/集体投资产品/银行业务的边界讨论，需慎重。

Q31：做衍生品（期货/杠杆）是否在 MiCA 内？
A：很多衍生品更可能落入 MiFID II/证券衍生品范畴而非纯 MiCA；需要法律边界判定与许可组合设计。

Q32：是否能只申请"面向专业客户"？
A：可以做客户分层，但仍要满足 MiCA 的客户保护、信息披露、投诉处理、利益冲突等基本义务；只是适当性/披露强度可按类别差异化。

Q33：可否只在斯洛伐克运营，不做护照？
A：可以；但仍建议在 BP 中写"未来护照路径"与材料可扩展性，减少后续二次大改。

Q34：护照通报需要准备什么？
A：通常需要：服务清单、目标成员国、分支/自由提供服务模式、当地营销与披露语言安排、投诉/ADR 接入安排、运营与外包可覆盖性说明。

Q35：平台是否需要"上币/下币委员会"？
A：强烈建议。监管会问：谁决策、谁评审、评分维度、利益冲突回避、紧急下架机制、重大事件处理与公告模板。

Q36：做市（Market Making）可以吗？
A：可以但必须高度披露并管理冲突：自营与客户撮合的顺序公平、信息隔离、禁止抢跑、异常行情处置、客户费用与滑点披露。

Q37：是否需要"最佳执行（Best Execution）"？
A：若涉及代客执行/经纪性质服务，监管通常会问"公平执行/最佳执行政策"、报价来源、路由逻辑、滑点与失败处理。

Q38：是否需要交易监控（Market Surveillance）？
A：平台/活跃交易业务通常需要。监管会问：操纵、刷量、关联账户、异常波动、内幕信息墙与调查流程。

Q39：不同服务组合会影响资本要求吗？
A：会。MiCA 通常采用"最低资本门槛 + 固定开支/审慎保障取高"思路，服务越重（平台/托管）资本与合规成本越高。

Q40：申请时能否把某些高风险服务排除？
A：可以。策略上建议把服务拆成"第一阶段可获批组合 + 第二阶段增项组合"，并在制度与系统设计中预留扩展接口。

Q41：需要提交"服务映射表"吗？
A：强烈建议提交：产品—流程—MiCA 服务条款—制度章节—系统控制点—证据附件编号，一张表让监管一眼看懂。

Q42：能否用"白标平台"快速满足平台要求？
A：可以但要证明控制权仍在你：参数、风控规则、日志导出、权限管理、审计与取证、供应商治理与退出迁移。

Q43：做钱包（非托管）是否需要 CASP？
A：取决于是否提供 MiCA 定义的服务实质；"非托管"也可能仍触发转移服务、客户交互、营销披露与风险提示义务，需做边界判断。

Q44：如何解释"custody vs technology provider"？
A：关键在于你是否控制客户密钥/资产转移权限；若你控制或共同控制（多签/MPC），监管通常按托管类要求审查。

Q45：申请组合的最佳实践是什么？
A：**先把最难模块（托管/平台）做成"可演示证据链"原型**，再决定是否纳入首批申请；否则材料写得再好也会在系统验证处被打回。

C. 申请前沟通、材料形态与项目节奏（Q46–Q60）

Q46：申请前应该做哪些准备？
A：至少完成：服务清单与映射、组织与岗位到位、资本与现金流模型、AML/Travel Rule SOP、ICT/外包治理、客户披露与协议包、证据链目录。

Q47：NBS 是否有申请前问卷/沟通渠道？
A：NBS 在"申请前准备"页面给出操作指引（包括问卷与附件提交方式及联络邮箱等）。

Q48：什么叫"可审计、可补件"的材料体系？
A：每条监管要求都能对应：条款依据 → 你的制度章节 → 你的流程/系统控制点 → 证据（日志/报表/截图/合约条款）→ 附件编号与页码。

Q49：为什么监管喜欢"ITS 表格化 + Index 索引"？
A：因为能快速核对信息要素，减少主观叙事；补件也能精准定位"缺哪个字段/哪个证据"。

Q50：最推荐的项目里程碑节奏？
A：差距评估 → 申请包成型（BdP/CMVM 类似双口径思路可借鉴）→ 证据链演示 → 递交 → RFI 迭代 → 面谈 → 获批 → 护照通报。

Q51：能否"先递交再补制度"？
A：不建议。NBS 25 工作日会看"完整性"；材料不完整会直接拖慢起算点与补件成本。

Q52：申请包通常分几册更清晰？
A：建议至少分 6 册：公司与治理、业务与流程、资本与财务、AML/Travel Rule、ICT/DORA、外包与客户披露（并做统一 Index）。

Q53：证据链最关键的"系统类证据"有哪些？
A：权限矩阵、关键操作日志（不可篡改）、KYC/EDD 工单、交易监控告警闭环、Travel Rule 报文/字段、钱包签名流程、对账与差异处理、事件演练记录。

Q54：监管会要求现场检查吗？
A：可能。尤其是实质运营、关键岗位履职、系统可调取性与记录留存；所以要准备"现场调阅清单"和快速导出能力。

Q55：是否需要面谈？
A：实践中高度可能。面谈通常围绕：治理问责、资金来源与股东适当性、AML/制裁/Travel Rule、平台/托管安全、外包控制权、财务可持续。

Q56：面谈怎么准备最有效？
A：把"条款—制度—流程—证据"做成 Q&A 卡片；让每个关键岗位能用同一口径解释并能现场演示系统与报表。

Q57：RFI（补件）最常见主题有哪些？
A：Substance、SoF/SoW、外包合同条款（审计权/退出/监管访问）、日志与权限、Travel Rule 实现、交易监控规则、资本与压力测试。

Q58：如何写 RFI 应答更容易通过？
A：统一格式：监管问题 → 条款依据 → 我方结论 → 改进措施 → 附件编号/证据 → 责任人 → 完成日期（闭环）。

Q59：是否要准备多语言材料？
A：至少准备英文为主；如面向零售客户，客户披露与协议往往需要当地语言版本与一致性控制。

Q60：能否边运营边申请？
A：高度敏感。未授权经营风险极高；建议在业务开展前完成许可路径设计，避免触发监管红线与后续信誉风险。

D. 实质运营、治理、人员、资本与股东（Q61–Q90）

Q61：什么是"实质运营（Substance）"？
A：监管要求你在斯洛伐克/欧盟内具备有效管理与可监管的运营实体：决策链、关键控制职能、数据与系统可调取、外包可控、应急可执行。

Q62：最低可解释的 Substance 组织长什么样？
A：至少：管理层（CEO/COO 或 GM）、合规负责人、MLRO、IT 安全负责人（可外包但必须内部有人负责监督），并能证明日常履职与决策留痕。

Q63：什么证据能证明不是"空壳公司"？
A：办公场地与租赁、工位与门禁、雇佣合同与值勤安排、会议纪要、权限矩阵、关键系统账户归属、供应商管理记录、监管调阅演练记录。

Q64：什么是"三道防线"？
A：一线业务自控、二线合规/风险监督、三线内审/独立审查；监管重点是"能否问责、能否独立制衡、能否整改闭环"。

Q65：小公司可以没有内审吗？
A：可以外包独立审查替代，但必须保证独立性、年度计划、抽样测试、缺陷评级与整改跟踪闭环。

Q66：关键岗位会被问哪些"必问题"？
A：合规：披露/营销/冲突/投诉；MLRO：KYC/EDD/STR/制裁/Travel Rule；IT 安全：权限/日志/事件/灾备；管理层：资本、外包、退出计划。

Q67：资本要求怎么理解?
A：核心逻辑是"最低资本门槛 + 持续审慎保障（常与固定开支/风险规模相关）取高"；必须证明持续经营与现金流可承受合规成本。

Q68：为什么监管会追问现金流?
A：因为很多机构资本写得够，但实际合规支出（KYC、链上分析、Travel Rule、SOC/SIEM、审计、渗透测试）无法长期承担，导致运营失控。

Q69：需要准备哪些财务报表?
A：至少 3 年 P&L、资产负债表、现金流量表，包含压力情景（市场波动、安全事件、增长不达预期、费用上升）。

Q70：股东 10%/重大持股要做什么?
A：做适当性审查：穿透到自然人 UBO、声誉与制裁筛查、财务稳健、资金来源/财富来源证据链、控制权与协议安排披露、持续变更通知机制。

Q71：SoF 与 SoW 区别?
A：SoF（Source of Funds）是"本次入资资金从哪来"；SoW（Source of Wealth）是"整体财富如何形成"。监管通常要求两者逻辑一致、证据可审计。

Q72：股东资金来源常见可接受类型?
A：薪酬分红、企业利润、投资收益、资产出售等；关键是"可解释 + 可证明 + 可追溯（银行流水/完税/审计/交易记录）"。

Q73：加密资产收益能作为资金来源吗?
A：可以但审查更严：需要交易所对账、链上地址证明、税务解释、资金从链到银行的合规路径与反洗钱解释。

Q74：股权结构复杂怎么做最清晰?
A：三张图：集团结构图（股权与控制权）、资金路径图（每一跳）、关联关系图（项目方/做市/供应商/客户渠道）。

Q75：董事/高管的核心要求是什么?
A：有效管理（effective management）与胜任力：能理解并落地 MiCA 要求、能监督外包与风险、能对重大事件与客户保护负责，并有值勤与授权链。

Q76：管理层在欧盟外是否可行?
A：高度不建议。监管容易认为决策不在本地，Substance 不成立。

Q77：合规与 MLRO 可以同一人吗?
A：小公司可能出现兼任，但要证明资源足够、冲突可控、汇报线独立，并避免与销售/业务 KPI 绑定。

Q78：信息安全负责人必须是全职吗?
A：可外包，但必须有内部责任人（信息安全官/系统负责人）能监督供应商、掌握权限与日志导出、组织演练与整改闭环。

Q79：是否要建立委员会（风险/审计/合规）?
A：按规模可简化，但必须有等效机制：重大事项审批、冲突回避、外包评估、年度合规与审计计划审批。

Q80：治理文件常见必备有哪些?
A：治理章程、授权矩阵（DoA）、冲突政策、风险偏好与风险登记册、董事会纪要模板、合规年度计划、投诉与申诉机制。

Q81：什么是"持续通知义务"?
A：股权/控制权变化、关键岗位变更、重大外包、重大事件、安全事故等触发事项，需要按监管口径及时通知/备案/申请批准。

Q82：被问到"你们如何管理利益冲突？"怎么答?
A：给制度 + 给流程 + 给证据：冲突登记册、关联交易审批、员工交易政策、礼品招待、信息隔离墙、回避机制、披露与复核记录。

Q83：被问到"你们如何保护客户资产？"怎么答?
A：说明资产隔离（链上地址/账务/权限）、对账频率与差异处理、转出控制（白名单/延迟/多签审批）、赔付边界、保险/保障（如有）、应急与迁移。

Q84：是否要做"客户分类（零售/专业）"?
A：建议做。因为披露强度、适当性/合适性、营销规则、风险提示与限制会随客户类别差异化。

Q85：是否要做员工胜任力框架?
A：建议建立：岗位胜任力矩阵、培训计划、测评题库、年度复训、关键岗位面谈脚本统一口径。

Q86：监管会看"合规资源预算"吗?
A：会。尤其平台/托管类，预算不足会被认为不可持续经营。

Q87：资本到位证明通常怎么做?
A：注册资本/实缴证明、银行入资凭证、验资（如适用）、资本来源解释与股东承诺函（必要时）。

Q88：什么是"资本补充机制"?
A：触发条件（亏损、增长、风险暴露上升、安全事故等）+ 增资路径/股东承诺/融资安排 + 时间表与责任人。

Q89：监管最不喜欢的股东情形有哪些?
A：资金来源无法解释、结构不透明、存在制裁/负面新闻未处置、项目方/做市商控制治理、以高杠杆收购且无资本缓冲。

Q90：如何降低 Fit & Proper 风险?
A：提前做"自查尽调包"：刑事/监管记录、诉讼与破产、制裁与负面新闻、税务居民、资金路径、关联关系；并把处置结论与复核记录固化。

E. AML / Travel Rule / 客户披露 / 系统证据链（Q91–Q120）

Q91：AML/CFT 交付的核心不是"手册"，是什么？
A：是一套可运行体系：风险评估→KYC/EDD→制裁/PEP→交易监控→调查闭环→STR 机制→培训→独立审查→记录留存。

Q92：Travel Rule（TFR）要求你做什么？
A：对加密资产转账随行信息进行采集、传递、校验、留存与异常处置；并能证明字段齐全、流程可回放、拒绝/延迟/人工复核有规则。

Q93：Travel Rule 是否只影响"转账服务"？
A：不仅。托管、交易平台、出入金、与其他 CASP 互转的场景都会被问到，因为涉及信息随行与对手方合规。

Q94：没有拿到对手方信息怎么办？
A：必须有 SOP：补采、退回、延迟、人工复核、拒绝、上报（如触发可疑），并保留证据链。

Q95：交易监控要做到什么程度？
A：要能解释规则库（阈值/场景）、告警分级、调查记录、结论与复核、STR 决策与时效，并能导出审计轨迹。

Q96：链上分析工具可以外包吗？
A：可以，但公司必须掌握：规则配置权、风险评分解释权、告警处置权、日志导出与审计权，不能"工具替你做决定"。

Q97：STR（可疑交易报告）要怎么"可审计"？
A：要有：触发→调查→结论→MLRO 决策→提交→回执→后续监控→复盘整改的闭环档案（含时间戳与责任人）。

Q98：制裁筛查的常见"被问点"有哪些？
A：名单来源、更新频率、命中处置、误报复核、账户冻结/限制、与 Travel Rule 字段一致性、与链上高风险地址联动。

Q99：客户保护与披露要交付哪些文件？
A：客户协议（T&Cs）、风险披露、费用披露、执行/报价政策、托管条款（如适用）、投诉机制、营销合规政策、利益冲突披露。

Q100：监管为什么强调"写给客户看的合规"？
A：因为披露与营销最容易出误导与争议；ESMA 也对"混同宣传"发出警示，监管会看你内部审核与发布流程。

Q101：营销材料需要审批吗？
A：需要制度化：谁起草、谁合规审查、谁批准、留存版本、投放渠道、受众分层、KOL/代理佣金与冲突披露。

Q102：平台类客户披露要特别写什么？
A：订单类型与撮合规则、异常行情与暂停机制、费用与滑点、风险提示、上币/下币规则、争议与纠错、市场滥用防控提示。

Q103：托管类客户披露要特别写什么？
A：密钥控制与签名方式、资产隔离、冻结/扣划边界、硬分叉/空投处理、转出审批与延迟、对账与差异处理、赔付与责任边界。

Q104：系统证据链最核心的"三张图"是什么？
A：系统架构图（业务流/数据流/权限流）、组织架构与汇报线图、外包与供应链图（含关键供应商与数据路径）。

Q105：权限管理要做到什么颗粒度？
A：RBAC 最小权限、特权账号管控、双人复核、关键操作强审计日志、定期权限复核与离职回收。

Q106：日志需要什么特性？
A：不可篡改、可检索、可导出、留存周期符合要求、能关联到工单/审批/交易记录，满足监管调查与内部审计。

Q107：渗透测试/代码审计必须吗？
A：高度建议。监管常要求你提供测试报告与整改闭环证据，尤其平台/托管/钱包系统。

Q108：事件响应要准备什么？
A：事件分级、响应流程、对内对外通报、取证与根因分析、补救与复盘、演练记录与改进计划。

Q109：BCP/DR（灾备）要提供什么？
A：RTO/RPO、备份与恢复策略、演练计划与演练结果、关键供应商故障应对、客户沟通模板。

Q110：外包治理为什么会被反复追问？
A：因为监管担心控制权外移。必须证明：审计权、监管可访问、数据权属、分包限制、事件通报、退出迁移可执行。

Q111：如何证明"退出计划"可执行？
A：提供 Wind-down Plan：触发条件、客户资产清退/迁移、对账与争议处理、公告与客服话术、数据封存、第三方替换与时间表。

Q112：客户投诉机制要做到什么？
A：受理→分级→调查→回复→升级→结案→统计复盘→整改闭环；并保留工单、录音、邮件与决策证据。

Q113：ADR（替代争议解决）要准备吗？
A：建议在条款中写清投诉渠道与升级路径，并准备跨境客户的语言支持与响应 SLA。

Q114：定价与费率为什么要写得很细？
A：因为费用披露与公平执行直接关联客户保护与投诉风险；监管会问"费用如何计算、何时变更、如何通知"。

Q115：压力测试要怎么做才"监管可读"？
A：明确情景（行情崩盘、黑天鹅、安全事件、外包中断）、假设、影响（收入/成本/资本）、缓释措施与触发增资机制。

Q116：最常见 AML 不通过点是什么？
A：风险评估空泛、EDD 触发器不清、交易监控无法解释、STR 档案不完整、制裁处置不闭环、Travel Rule 只是口头承诺。

Q117：最常见 IT 不通过点是什么？
A：权限不清、日志不可导出、密钥管理不合规、没有演练证据、供应商条款缺审计权/退出、事件响应不可执行。

Q118：最常见客户披露不通过点是什么？
A：宣传夸大或混同受规管/不受规管产品；风险披露不可理解；费用不透明；暂停/冻结/纠错条款不清；投诉路径不明确。

Q119：怎样最快提升"通过率"？
A：把制度写成 SOP，把 SOP 做成系统控制点，把控制点固化成证据链（日志/报表/工单/签批），并做 Index 交叉引用。

Q120：仁港永胜的交付打法是什么？
A：以监管审查路径为主线：**服务映射 → 双线材料（审慎/行为） → 系统证据链 → RFI 闭环包 → 面谈题库**，把"能运营"证明给监管看。

F. AML/CFT 体系（含制裁、PEP、链上风险）Q121–Q160

Q121：AML 风险评估（Enterprise-wide Risk Assessment, EWRA）必须写到什么颗粒度？
A：至少要做到“可重复计算、可复核”的方法论：

- **风险维度**：客户类型（零售/专业/机构）、产品与服务（平台/托管/转移/OTC/做市）、渠道（线上/代理/KOL）、地域（高风险辖区）、交易行为（高频/拆分/混币）、交付方式（自托管/托管）、外包依赖（KYC/链上分析/Travel Rule 供应商）。
- **评分逻辑**：权重、阈值、分层结果（低/中/高）、触发 EDD 规则与限制措施。
- **治理**：年度复核、重大事件触发复核、董事会批准、版本控制。
- **证据链**：评分表、会议纪要、复核记录、变更记录（Change Log）。

Q122：监管会如何验证你们的风险评估不是“写出来的”？
A：看你能否把风险评估落到可运行控制：

- 风险分层是否驱动 **KYC/EDD 深度、限额、监控阈值、人工复核比例**；
- 监控规则库是否与风险分层一致；
- EDD 结论是否会触发“禁止/限制/增强监控/定期复核”；
- 是否能导出样本客户的“风险分数→触发器→处置→复核”全链条记录。

Q123：客户尽调（CDD）最低信息集一般需要哪些？
A：按“可识别+可验证+可持续更新”的口径：

- 自然人：身份证明、住址证明、联系方式、税务居民信息（含自证）、职业/雇主、资金来源概要、预期交易行为。
- 法人（KYB）：注册文件、董事/授权签字人、股权结构与 UBO 穿透、经营资料、业务性质、资金来源、控制权说明。
- 共通：制裁/PEP/负面新闻筛查结果、风险评分、同意条款与风险披露确认（留痕）。

Q124：什么情况必须做 EDD（增强尽调）？
A：建议以“触发器清单 + 处置矩阵”交付：

- PEP/高风险关联方；
- 高风险辖区/受制裁辖区关联；
- 资金来源无法合理解释或高度依赖现金/第三方代付；
- 使用混币器、匿名增强工具、可疑链上聚合/跳转；
- 异常交易模式（拆分/快进快出/对倒/自成交/关联账户集群）；
- 代理/OTC 场景的非面对面高风险客户；
- 高额或高频转账、与未受监管 VASP 或自托管地址高风险互动。

Q125：PEP 命中就必须拒绝吗？
A：不必“一刀切”，但必须：更高层级审批、资金来源/财富来源加强、持续监控增强、定期复核更频繁；并对命中与误报复核留存证据。

Q126：制裁筛查需要覆盖哪些名单与频率？
A：必须保证覆盖主要制裁名单与本地监管期望（常见包括联合国、欧盟、OFAC 等），并做到：**实时/准实时筛查 + 名单更新记录 + 命中处置 SOP + 误报复核**。关键是“你用什么数据源、多久更新一次、谁负责、如何留痕”。

Q127：负面新闻（Adverse Media）筛查怎么做才合规？
A：不是“搜一下 Google”。你要交付：

- 筛查范围（诈骗、洗钱、恐怖融资、制裁规避、腐败、金融犯罪）；
- 来源与工具（供应商或内部流程）；
- 评级与处置（低/中/高、是否触发 EDD/拒绝/限制）；
- 复核与结论（谁复核、依据是什么、何时复核）。

Q128：链上分析（Blockchain Analytics）是必须的吗?
A：对多数涉及转账/托管/平台的 CASP，监管实践上非常倾向要求具备链上风险识别能力。即使外包，也必须保持：规则配置权、解释权、审计权、数据导出能力。

Q129：如何把链上风险“写成监管可读”？
A：用“场景库”写法：

- 场景：混币器/暗网/诈骗地址/高风险交易所/受制裁地址/跨链桥风险/集群地址；
- 输入：地址/TxHash/标签/风险评分；
- 决策：阻断/延迟/人工复核/上报；
- 留痕：告警截图、调查笔记、结论与复核、STR 决策。

Q130：交易监控（Transaction Monitoring）规则库要怎么交付?
A：建议输出“规则库总表 + 20–60 个重点场景”的交付版：

- 规则名称、阈值、适用客户层级、触发逻辑、例外情况；
- 告警分级（P1–P3）、响应 SLA、升级路径；
- 调查步骤（要看哪些数据、要问哪些问题）；
- 结案标准、复核要求、是否触发 STR。

Q131：告警调查（Case Management）要有什么证据?
A：监管喜欢“可回放”证据链：

- 告警 → 分派 → 调查 → 信息补充 → 结论 → 复核 → 关闭；
- 每一步时间戳、责任人、附件（链上图谱/对账/聊天记录/客户解释）。
- 可导出样本（至少 10 个案例）用于监管抽样。

Q132：STR/SAR 的决策机制如何设计?
A：必须明确 MLRO 的独立决策权：

- 触发 STR 的典型模式（规则命中、人工发现、外部线索、制裁命中）；
- 决策会签（必要时合规/法律支持），但不应被业务否决；
- 提交与回执归档；
- 事后加强监控与账户处置；
- 年度统计与复盘。

Q133：是否需要 CTR（大额交易报告）？
A：取决于当地 AML 框架是否规定强制大额报告阈值与类型。即使没有强制 CTR，监管仍可能期待你对“大额/异常”有更强监控与调查机制，并能解释阈值设置依据。

Q134：可疑交易与客户资产冻结怎么处理?
A：要有“冻结/限制”策略：

- 冻结触发条件；
- 冻结权限（谁能冻结、是否双人复核）；
- 对客户通知策略（避免 tipping-off 的风险）；
- 与 FIU/监管沟通与记录；
- 解冻条件与审批链。

Q135：如何避免“tipping-off（通风报信）”风险?
A：制度层面写清：当进入 STR 评估/提交流程时，客服对客户的回复模板、内部沟通范围、信息访问权限与日志留存要求。

Q136：AML 培训需要做到什么?
A：建议用“岗位分层 + 年度计划 + 测试题库 + 通过标准 + 留痕”：

- 全员基础培训；
- 高风险岗位（客服、KYC、交易监控、OTC）强化培训；
- MLRO/合规/管理层专题培训；
- 每次培训记录、测试成绩、补训安排。

Q137：独立审查/内审（AML Audit）怎么做?
A：至少年度一次独立审查：抽样 KYC、EDD、告警、STR、制裁命中处置、Travel Rule 档案；输出缺陷评级、整改计划、复核结论与董事会汇报记录。

Q138：可否完全依赖供应商完成 AML?
A：不行。你可以外包工具，但不能外包责任与决策。监管要看到你对规则库、阈值、风险偏好、STR 决策拥有主导权与可解释性。

Q139：如何处理“代理/KOL 引流”带来的 AML 风险?
A：必须把代理纳入 AML 生态：

- 代理准入尽调（KYC/KYB/制裁/负面新闻）；
- 佣金结构与异常激励控制；
- 代理营销话术审查；
- 代理客户质量监控（退单率、投诉率、可疑率）；
- 终止与追责条款。

Q140：如何处理“自托管地址（unhosted wallet）”风险?
A：必须有策略：地址风险评分、所有权证明（可选）、转账限额、强化监控、Travel Rule 异常处理、必要时拒绝或延迟交易，并留存决策记录。

Q141：AML 与平台市场监测（Market Surveillance）有什么区别?
A：AML 侧重洗钱/恐怖融资/制裁；市场监测侧重操纵、刷量、内幕、对倒等市场行为。但两者会共享数据与案例，建议建立协同机制与升级路径。

Q142：是否需要“集团统一 AML 政策”？
A：可有集团框架，但必须本地化：斯洛伐克实体的风险评估、阈值、报告路径、FIU 沟通机制必须明确，不能完全依赖母公司。

Q143：如何证明 AML 体系“可运行”？
A：交付 3 类证据：

1. 制度与 SOP（可审计版本控制）；
2. 系统证据（工单、日志、告警、STR 档案）；
3. 样本演示（抽样客户/交易全链路）。

Q144：AML 数据与隐私（GDPR）如何兼容?
A：要写数据治理：数据最小化、访问控制、留存周期、数据出境与第三方处理协议、监管调阅机制、数据主体权利与 AML 例外的平衡说明。

Q145：NBS 更关注 AML 的哪些点?
A：实践上通常会聚焦：风险评估是否驱动控制、STR 决策独立性、制裁与 Travel Rule 运行证据、外包治理与数据可调取性。

Q146：最常见 AML 补件点有哪些?
A：EDD 触发器不清、规则库不具体、告警闭环缺证据、STR 档案模板缺、制裁命中处置与冻结策略不完整、Travel Rule 只是“承诺”。

Q147：如何构建“制裁/AML 红线清单”？
A：把不可接受行为列为红线：

- 与受制裁主体/地址持续交易；
- 未核实 UBO/身份；
- 明显可疑仍放行且无调查记录；
- STR 触发后仍向客户透露；
- 监控规则故意关闭/绕过。
  并建立违规升级与纪律处分机制。

Q148：AML 政策至少应包含哪些章节?
A：建议 12–18 章：风险评估、KYC/KYB/UBO、EDD、制裁/PEP、交易监控、链上分析、STR、记录保存、培训、独立审查、代理管理、TFR（如合并）等。

Q149：记录保存年限怎么设?
A：按 AML/监管要求设置（通常较长）。关键是：留存范围明确、可检索、可导出、不可篡改、访问权限与审计轨迹完善。

Q150：如何把“风控、AML、合规”做成一套体系?
A：用统一的 Case Management 平台或统一编号：客户编号—账户编号—告警编号—工单编号—STR 编号—投诉编号可互相追溯，监管抽样时非常加分。

Q151：可疑地址标签来自供应商，监管会认可吗?
A：认可“工具”，但仍要求你能解释：标签来源可靠性、误报复核流程、最终决策责任在谁。

Q152：如何处理“跨链桥/Layer2”带来的识别困难?
A：要写明方法：支持的链与桥、风险评分策略、无法识别时的限制策略（限额/延迟/人工复核/拒绝），并披露给客户。

Q153：若提供“转账服务”，AML 与 TFR 谁先谁后?
A：建议并行：

- 先做客户身份与风险评分；
- 发起转账前完成必要字段采集与对手方检查；
- 转账后进行交易监控与异常处置；
- 任何一环不足都要触发延迟/人工复核/拒绝。

Q154：如何设置“阈值”才合理?
A：阈值应基于：风险评估结果、客户分层、历史数据、行业基准与压力测试。并保留“阈值调整记录”与董事会/合规审批记录。

Q155：AML 系统上线前是否要做 UAT/演练?
A：强烈建议。输出：测试用例、测试结果、缺陷修复记录、上线审批记录。

Q156：如何应对监管要求“抽样展示”某个 STR 案例?
A：你需要 STR 档案包：触发原因、链上/链下证据、客户解释、调查日志、MLRO 决策、提交回执、后续监控与账户处置结论。

Q157：客户拒绝提供 EDD 信息怎么办?
A：制度必须写清：拒绝 EDD → 限制/拒绝服务 → 必要时提交 STR（视情况）→ 留存拒绝记录与沟通证据。

Q158：如何处理“同一 UBO 多账户/关联账户集群”?
A：要有关联账户识别逻辑：同设备、同 IP、同收款地址、同法人控制、同代理来源等；并在监控规则中体现“集群风险”。

Q159：AML 体系如何与财务对账协同?
A：对账差异可能是欺诈/内部风险信号。建议把对账差异纳入监控：大额差异、频繁冲正、异常手续费返还、员工异常操作等。

Q160：AML 最终的“交付验收标准”是什么?
A：监管视角的验收标准：**能运行、能解释、能导出、能复盘**。你要随时拿出客户样本与交易样本，完整回放端到端证据链。

G. Travel Rule（TFR）端到端落地 Q161–Q175

Q161：Travel Rule（TFR）最核心的合规目标是什么?
A：确保加密资产转账随行信息在 CASP 之间传递、校验、留存，并具备异常处理机制。TFR 是欧盟统一法规，属于硬性合规模块。

Q162：TFR 信息字段通常分哪几类?
A：通常涉及：发起人（Originator）、受益人（Beneficiary）、发起/受益 CASP、账户/钱包标识、地址信息、交易标识、必要的身份信息与参考号等。关键是：你要写明“你采集哪些字段、何时采集、如何验证、如何留存”。

Q163：Travel Rule 适用哪些场景?
A：至少包括：CASP ↔ CASP 转账；客户 ↔ CASP 提币/充币（取决于场景与对手方性质）；与自托管钱包交互时的信息采集与风控策略也是监管常问点。

Q164：如果对手方 CASP 不支持 Travel Rule 通道怎么办?
A：必须有策略：

- 对手方识别（是否受监管/是否支持通道）；
- 信息不足时的处理：延迟、退回、人工复核、拒绝；
- 高风险对手方名单与限制；
- 全过程留痕（重要）。

Q165：如何证明 Travel Rule “可运行”?
A：用 3 类证据：

1. 报文字段样本（去敏后）；
2. 系统流程截图/日志（采集→发送→接收→校验→存档）；
3. 异常案例（字段缺失/对手方拒绝/不一致）的处置工单与结论。

Q166：Travel Rule 与 AML 调查如何联动?
A：字段不一致、对手方信息异常、频繁失败重试、对手方高风险辖区，均应触发 AML 告警与加强监控。

Q167：Travel Rule 数据保存怎么做?
A：必须可检索、可导出、与交易记录一一对应，并设置访问控制与审计日志。保存期按法规与监管预期设定。

Q168：自托管钱包场景如何处理 Travel Rule?
A：监管通常会要求你至少具备：地址风险评分、所有权合理验证（可选）、限额与延迟、增强监控、必要时拒绝，并披露给客户。

Q169：Travel Rule 供应商可以外包吗?
A：可以，但必须满足外包治理：审计权、监管访问、数据权属、分包限制、事件通报、退出迁移。并且你要能解释字段映射与异常处置规则，不能“供应商说合规就合规”。

Q170：Travel Rule 失败率过高会有什么风险?
A：监管会认为你无法持续合规运营：信息随行不完整意味着 AML/制裁风险显著上升。必须有 KPI（成功率/异常率/人工复核时效）与治理机制。

Q171：Travel Rule 与隐私（GDPR）冲突吗？
A：不应视为冲突，而是数据治理问题：最小必要、访问控制、留存周期、处理者协议、数据主体权利与 AML 例外边界说明。

Q172：Travel Rule 的“拒绝/退回”需要客户同意吗？
A：需在客户协议与披露中提前写明：当信息不足或风险过高时可拒绝/延迟/退回，并说明费用与处理时限。

Q173：如何做 Travel Rule 的日常监控？
A：建议建立仪表板：成功率、失败原因分布、对手方支持情况、人工复核 backlog、超时案件、异常对手方名单更新。

Q174：Travel Rule 的演练需要做吗？
A：强烈建议做“桌面演练 + 系统演练”：对手方故障、字段不一致、安全事件、数据泄露，输出演练记录与改进清单。

Q175：TFR 模块最常见补件点有哪些？
A：字段定义不清、无法展示端到端流程、异常处置缺 SOP、对手方识别缺机制、留存与检索能力不足、外包合同缺审计权与退出条款。

H. 客户保护、披露、营销与公平执行 Q176–Q200

Q176：客户保护为什么是 MiCA 审查重点？
A：MiCA 的核心之一是客户资产保护、信息披露与市场诚信。监管会把它视为“能否面向零售客户”的门槛。

Q177：客户披露（Disclosure Pack）最少包含什么？
A：至少四件套：

1. 风险披露（价格波动、技术风险、托管风险、法律风险）；
2. 费用披露（费率、价差、第三方费用、变更通知机制）；
3. 执行/报价政策（报价来源、滑点、失败处理）；
4. 投诉机制（渠道、时限、升级、ADR）。

Q178：营销合规最常见雷区是什么？
A：误导性表述：

- 把“受监管主体”泛化到不受监管产品；
- 暗示保本/固定收益；
- 夸大牌照覆盖范围或“全欧盟通行无需本地合规”；
- 未披露风险与费用；
- KOL/代理夸大宣传未管理。

Q179：如何建立营销审批流程？
A：建议制度化：起草→合规审查→管理层批准→版本控制→投放记录→抽检与复盘。并规定禁用词库与强制风险提示模板。

Q180：客户适当性/合适性在 MiCA 下如何处理？
A：取决于服务性质。若涉及投顾/组合管理或复杂产品，应建立客户知识测评、风险承受能力评估、产品分层、强提醒与拒绝销售机制，并留存测评与告知证据。

Q181：费用怎么披露才算透明？
A：不仅写费率，还要写：计费时点、计费基础（成交额/名义金额）、示例算式、可能产生的第三方费用、费率变更通知周期、对账单展示方式。

Q182：平台类业务的“公平执行”怎么写？
A：至少包括：订单优先级、撮合规则、异常行情处置、暂停/熔断、交易失败处理、客户通知机制、内部员工交易限制与冲突管理。

Q183：滑点（slippage）与异常报价如何处理？
A：要有政策：报价来源、聚合逻辑、异常过滤、滑点阈值、客户确认机制（必要时）、争议处理与补偿规则。

Q184：如何处理客户资产冻结/限制与客户告知？
A：披露中要写清：冻结触发条件（制裁/可疑/司法/技术风险）、冻结权限与审批链、通知方式（避免 tipping-off 的例外）、申诉渠道与处理时限。

Q185：如何处理硬分叉/空投/链上事件？
A：披露必须明确：是否支持、支持条件、资产归属、技术风险、对账与分配流程、客户通知与争议处理。

Q186：客户协议（T&Cs）最常缺哪几条？
A：常缺：

- 服务边界与不提供内容（排除项）；
- 费用与变更通知；
- 暂停/终止、强制平仓（如有）；
- 托管责任与赔付边界；

- 投诉/ADR/司法管辖；
- 数据使用与隐私、监管披露条款。

Q187：零售客户风险提示如何写更“监管友好”？
A：要求：清晰、可理解、不可被营销文字淹没；并强制客户确认（点击确认/签署），保存确认日志。

Q188：是否需要“客户对账单/交易回单”？
A：强烈建议。监管会问客户是否能核对交易、费用、余额变化；对账单也是投诉与争议处理的关键证据。

Q189：如何处理客户投诉的 SLA?
A：建议写三层：受理（T+0/T+1）、初步回复（T+3/T+5）、结案（T+15/T+30，视复杂度）；并定义升级路径与根因复盘机制。

Q190：ADR（替代争议解决）要怎么在条款中体现?
A：写清：何时进入 ADR、需要哪些材料、时限、语言支持、是否影响客户司法权利，并保留沟通证据。

Q191：KOL/代理推广必须披露什么?
A：至少披露：推广关系、佣金/利益关系、风险提示义务、禁止收益承诺。并要求 KOL 文案走合规审查。

Q192：面向其他欧盟国家营销时需要做什么?
A：即使护照通报，也需做“本地营销合规补丁”：语言、广告规则、消费者保护、投诉渠道、费用显示规则等，避免被落地国监管盯上。

Q193：如何避免“混同宣传”（regulated vs unregulated）？
A：建立产品清单与监管标签：每个产品标注适用许可、适用客户、风险等级；营销材料强制引用对应标签与风险提示。

Q194：若提供托管服务，客户资产隔离如何向客户解释?
A：披露要写明：链上地址/账户体系、账务隔离、权限隔离、对账频率、差异处置、审计安排、在极端情况下的处置顺序。

Q195：如何向客户披露“外包与第三方”风险?
A：披露应说明：关键服务可能依赖第三方（云/KYC/链上分析/Travel Rule），并说明你如何监督、如何确保数据安全、如何退出迁移。

Q196：客户数据是否会被共享给集团/第三方?
A：必须透明披露：共享目的、范围、法律依据、跨境传输机制、数据主体权利、监管调阅可能性，并与 AML 例外衔接。

Q197：是否需要“客户分类与限制策略”？
A：建议建立：零售/专业、低/中/高风险、地区限制、产品限制、限额策略，并把它写进风控与披露体系。

Q198：如何处理“价格异常导致客户损失”的争议?
A：要有纠错与补偿机制：异常识别标准、暂停交易、回滚/冲正条件、客户通知、补偿原则、升级审批与记录。

Q199：客户资金（法币）如何保护?
A：若涉及法币出入金，必须设计客户资金隔离账户、对账机制、第三方支付/银行合作治理、退款与纠错流程、反欺诈与 AML 控制。

Q200：客户保护模块最常见补件点有哪些?
A：风险披露不清、费用不透明、营销审查缺失、投诉机制不成体系、平台规则不完整、托管责任边界含糊、缺少客户确认留痕。

I. 外包治理、系统证据链、数据治理、退出与流程（Q201–Q240）

Q201：外包清单（Outsourcing Register）要怎么做?
A：必须建立完整外包台账：供应商、服务内容、数据类型、是否关键/重要外包、SLA/KPI、分包情况、审计权条款、退出计划、负责人、年度复核日期。

Q202：什么是“关键/重要外包”？
A：通常指：影响持续提供受规管服务、影响客户资产安全或关键数据处理的外包，如云、托管钱包、KYC、交易引擎、Travel Rule 通道、SOC/SIEM 等。

Q203：外包合同的“必备条款包”有哪些?
A：至少包括：

- 审计权（你与监管可审计/可取证）；
- 监管可访问性（监管检查时能调取数据/进入系统）；
- 数据权属与数据驻留（如适用）；
- 分包限制与披露；
- 事件通报时限与配合义务；
- 业务连续性与灾备要求；
- 退出/迁移（Exit）与交接支持；
- 终止权与违约救济。

Q204：如何做第三方尽调（TPRM）？
A：至少三类尽调：安全（ISO/SOC2、渗透测试、漏洞管理）、财务稳定性（持续经营能力）、合规与法律（资质、制裁、数据处理协议）。并保存年度复核记录。

Q205：外包退出计划要写多细?
A：要可执行：替代供应商名单、迁移步骤、时间表、数据导出格式、客户通知模板、回滚方案、演练安排。

Q206：供应链安全（Supply Chain Risk）如何写才有说服力?
A：写“控制点”：供应商准入、代码供应链（依赖管理）、密钥与证书管理、补丁与漏洞披露、重大事件通报与联动演练。

Q207：信息安全最关键的“可演示证据链”有哪些?
A：权限矩阵、特权账号审计、关键操作日志、密钥管理流程（多签/MPC/HSM）、渗透测试报告与整改、事件演练记录、BCP/DR 演练结果。

Q208：日志必须具备哪些属性?
A：不可篡改、时间同步、可检索、可导出、访问控制、留存期限、与工单/审批/交易记录可关联。

Q209：如何证明“密钥控制权在你手里”？
A：提供：签名流程图、角色与阈值（m-of-n）、审批链、应急密钥策略、密钥轮换、备份与灾备、冷/热钱包隔离、签名日志与审计记录。

Q210：托管与平台是否必须做对账?
A：必须。至少每日对账（更高频更好）：链上余额、内部账、客户余额、法币账户；差异处理 SOP、责任人、纠错与客户通知机制。

Q211：数据治理（含税务/报告导向）要交付什么?
A：建议三层：

1. 字段标准（KYC/交易/TFR/税务字段一致性）；
2. 留存与追溯（证据封存、日志策略、版本控制）；
3. 报告抽取（监管/税务/管理报表可自动生成，且可解释）。

Q212：记录保存（Recordkeeping）怎么写才不被补件?
A：明确：保存范围（KYC、订单、撮合、转账、告警、STR、投诉、外包评估、系统日志）、保存期限、存储介质、检索与导出、权限、销毁规则与审计记录。

Q213：客户删除数据（GDPR）请求如何处理?
A：必须写清：AML/监管留存的法定例外；哪些数据可删除、哪些必须保留；如何回应客户、如何留存处理记录。

Q214：财务模型与“可持续经营”证明要包含哪些关键假设?
A：客户增长、交易量、费率、成本（合规/安全/外包/审计）、人力成本、营销成本、坏账与欺诈损失（如有）、压力情景与资本补充机制。

Q215：监管最常质疑财务模型什么?
A：合规成本低估、收入假设过乐观、未考虑安全事件与外包事故成本、现金流缺口无补充方案、资本触发机制不清。

Q216：定价（Pricing）与费用变更如何合规?
A：要写：定价原则、费用展示方式、变更通知期、客户确认方式、对存量客户的适用规则、对账单展示字段。

Q217：有序退出（Wind-down Plan）必须包含什么?
A：触发条件、客户资产清退/迁移、对账与争议处理、平台关闭步骤、客服与公告模板、数据封存、供应商终止与迁移、人员与权限回收、监管通知机制。

Q218：BCP/DR 的监管期望是什么?
A：不仅写方案，还要有演练证据：RTO/RPO、恢复演练记录、供应商故障演练、关键岗位替补机制、通信与决策链。

Q219：重大事件通报机制需要写吗?
A：需要。定义重大事件、分级、通报时限、通报内容、根因分析、整改与复盘、客户通知原则，并能输出演练记录。

Q220：如何准备监管现场检查（On-site）？
A：准备“监管调阅清单”：KYC 样本、告警样本、STR 样本、TFR 样本、权限与日志导出、外包合同条款、董事会纪要、对账与差异处理记录。

Q221：ITS 表格化递交是什么意思?
A：指把申请信息要素按监管要求以结构化表格填报，并用附件编号与页码交叉引用，减少叙事型材料的歧义，提高补件效率。

Q222：如何做“Index 统一索引”？
A：建立总索引：字段/条款 → 文件名 → 章节 → 附件编号 → 页码/链接 → 负责人 → 版本号；并维护变更日志。

Q223：补件（RFI）常见结构怎么写?
A：推荐闭环写法：问题 → 条款依据 → 我方结论 → 改进措施 → 证据附件编号 → 责任人 → 完成日期 → 复核结论。

Q224：补件时最忌讳什么?
A：空口承诺、没有证据、附件编号混乱、前后口径不一致、把责任推给供应商、无法解释阈值与决策逻辑。

Q225：申请流程中“完整性检查”会看什么?
A：是否覆盖关键模块：服务清单与映射、治理与人员、资本与财务、AML/TFR、ICT/安全、外包治理、客户披露与投诉、记录保存与退出计划。

Q226：如何缩短整体周期?
A：提前把系统证据链跑通；把外包合同条款一次性修正到位；股东 SoF/SoW 做成可审计链；Index 做好，减少往返解释。

Q227：跨境护照通报在获批后怎么启动?
A：准备“护照通报包”：服务范围、目标成员国、运营模式、营销与披露语言安排、投诉渠道、外包可覆盖性、当地合规补丁清单。

Q228：如果业务要新增服务（例如从兑换扩到托管），怎么办？
A：通常属于变更/增项，需要重新证明资本、系统安全、客户资产保护、人员胜任力等已满足新增服务的要求，并准备更新后的制度与证据链。

Q229：关键人员更换会触发什么？
A：触发变更通知/批准（视岗位与影响），同时要更新岗位履历、JD、汇报线、权限、培训与交接记录，并保留董事会决议与值勤安排。

Q230：重大外包变更（更换云/托管/链上分析）怎么做？
A：要做外包重评估：风险评估、合同条款审核、迁移与退出计划、数据与日志连续性、演练记录、客户通知与监管沟通策略。

Q231：数据出境与跨境访问会被问吗？
A：会。要说明数据驻留、访问控制、跨境传输法律依据、第三方处理者协议、监管调阅机制与审计轨迹。

Q232：如何处理“集团共享服务中心”模式？
A：必须证明本地实体仍具控制权：关键决策、权限管理、数据调取、外包合同权利、监管检查配合都不能被母公司“卡脖子”。

Q233：如何设置 KPI/KRI 来治理合规与运营？
A：建议 KPI/KRI：告警处理时效、STR 数量与质量、Travel Rule 成功率、投诉率与结案时效、权限复核完成率、渗透测试整改完成率、对账差异率等。

Q234：如何证明治理“可问责”？
A：用“会议纪要 + 决议编号 + 附件索引”：关键决策（外包、阈值调整、上币/下币、重大事件处置）都有记录、责任人、时间戳与后续复核。

Q235：如何处理“异常事件导致暂停服务”的客户沟通？
A：准备预案：公告模板、FAQ、客服话术、工单处理与赔付策略、恢复时间预估口径（谨慎）、监管通报同步。

Q236：若发生安全事件（盗币/私钥泄露），第一时间做什么？
A：启动事件响应：隔离系统、暂停高风险操作、冻结可疑资产、取证、通知关键人员、按制度进行监管/客户通报评估、执行应急签名与资产迁移方案，保留全过程证据链。

Q237：如何将“退出计划”与“BCP/DR”区分写清？
A：BCP/DR 是“保持业务连续”；退出计划是“停止业务并保护客户”。两者触发条件、行动步骤与沟通对象不同，但共享对账、客户通知、数据封存等模块。

Q238：哪些内容建议在申请前做“演示环境（Demo）”？
A：建议至少能演示：开户/KYC、风险评分、告警调查闭环、TFR 报文、权限与日志导出、签名流程（模拟）、对账与差异处理、投诉工单。

Q239：监管为什么强调“可导出（exportable）”？
A：因为检查与调查需要快速调阅。不能导出日志/工单/报表会被认为不可监管，直接影响审批效率与持续监督信心。

Q240：本页模块最关键的交付结论是什么？
A：把合规做成“系统化证据链”而不是“文字承诺”：外包可控、日志可导出、TFR 可回放、AML 可闭环、客户披露可上线、退出可执行——这就是监管愿意批牌的底层逻辑。

J. 平台类业务（Trading Platform）规则 + 监测 + 证据链 Q241–Q280

Q241：申请“运营交易平台（Trading Platform）”与普通兑换/经纪最大的差异是什么？
A：平台类业务被监管视为“市场基础设施型能力”，审查重点从“你能否合规提供服务”升级为“你能否维持市场公平、透明与韧性”。差异主要体现在：

- **平台规则体系**（规则手册、订单类型、撮合、异常行情、停牌/熔断）；
- **市场监测能力**（操纵、刷量、自成交、关联账户、内幕信息墙）；
- **数据可审计**（订单簿、撮合日志、时间同步、不可篡改留痕）；
- **上币/下币治理**（评估、披露、持续监控、紧急下架）；
- **冲突管理**（自营/做市/上币项目方关系、费用与激励披露）。

Q242：平台规则手册（Rulebook）至少要包含哪些章节？
A：建议交付“监管可读版”Rulebook（20–40 章，可按规模裁剪）：

- 平台概览与角色定义（会员/客户/做市商/发行方等）
- 账户与权限、KYC 门槛与限制
- 订单类型与撮合优先级（价格/时间/其他）
- 交易时段、维护窗口、暂停机制
- 手续费与费用披露、费率变更机制
- 异常行情识别与处置（保护机制、熔断、回滚政策如适用）

- 市场滥用与操纵禁止条款、监测与处罚流程
- 上币/下币规则与披露
- 争议处理、投诉与 ADR
- 数据与记录保存、审计与监管调阅
- 重大事件通报、BCP/DR、退出计划摘要
- 责任边界与免责声明（合规口径）

Q243：撮合规则需要写到什么程度？
A：要写到“可复现”。监管常问：同价位多单如何排序、撮合引擎是否有人工干预、是否存在隐藏优先权。建议交付：

- 撮合优先级（价格/时间/比例）
- 部分成交逻辑、撤单逻辑
- 冻结余额与解冻机制
- 撮合日志字段（订单ID、时间戳、撮合ID、价格、数量、手续费）
- 时间同步（NTP）与不可篡改日志策略

Q244：平台是否必须公开订单簿深度/成交数据？
A：取决于平台模型与客户类型，但监管一般要求信息披露“足够让客户理解价格形成与执行质量”。至少要有：成交历史、价格曲线、费用、滑点解释、订单执行回单与对账。

Q245：平台如何处理“异常行情/闪崩”事件？
A：必须有可执行预案：

- 异常识别阈值（价格偏离、成交量异常、价差异常）
- 自动保护机制（暂停交易、提高保证金/限制下单，视模式）
- 人工升级路径（谁有权暂停、谁复核、谁通知）
- 客户通知模板与客服话术
- 事后复盘（根因、受影响客户、补救措施）
- 是否回滚/冲正的规则（如适用，需极慎重并写清条件）

Q246：平台需要“市场监测（Market Surveillance）”系统吗？
A：强烈建议具备。监管常把它视为平台类“必答题”。即便外包，也要保留：参数配置权、解释权、审计权、数据导出能力。

Q247：市场操纵识别要覆盖哪些典型模式？
A：至少覆盖：

- Wash Trading（刷量/自成交）
- Spoofing/Layering（挂撤单诱导）
- Pump & Dump（拉盘砸盘）
- Marking the close（收盘操纵）
- Cross-market manipulation（跨平台联动）
- Insider dealing（内幕）
- Collusion（关联账户合谋）
  并输出“场景→指标→阈值→处置→留痕”表格。

Q248：如何识别关联账户集群？
A：建议用多因子：设备指纹、IP、银行卡/地址复用、相同提现地址、相同推荐人/KOL、相同法人控制、相似交易行为。建立“集群评分”，触发限制与调查。

Q249：平台允许做市商（Market Maker）吗？
A：可以，但必须把做市纳入冲突管理与透明披露：

- 做市商准入标准与协议
- 做市商与平台关系披露（是否关联方）
- 做市行为限制（禁止操纵、禁止内幕）
- 做市奖励结构与费用返还披露
- 做市监测与处罚机制

Q250：平台自营交易（proprietary trading）允许吗？
A：可以，但监管会非常关注冲突：信息隔离、优先权、公平执行、客户损害风险。建议：

- 明确自营与客户交易隔离（人员、系统权限、信息墙）
- 自营交易披露与限制（不得抢跑，不得操纵）
- 审计轨迹与独立复核机制

Q251：上币（Listing）制度必须交付哪些文件?
A：建议交付“三件套”：

1. 上币政策（原则与流程）
2. 上币评估模板（评分表/尽调清单/风险披露）
3. 上币委员会章程（成员、回避、决议、紧急下架机制）
   并附样例：1–3 个假想项目的评估演示（去敏）。

Q252：上币评估维度一般包括什么?
A：建议至少覆盖：项目治理与团队、技术安全（审计/漏洞）、代币经济模型、市场操纵风险、法律合规与制裁风险、链上集中度、黑客/诈骗历史、信息披露质量、持续监控与下架触发器。

Q253：紧急下架（Emergency Delisting）触发器怎么定义?
A：典型触发：重大安全漏洞、监管禁令、明显诈骗证据、链上异常（大量盗币）、市场操纵严重、项目方失联/重大虚假披露。必须写清客户通知、资产处置与争议处理。

Q254：平台需要“内部信息墙（Chinese Wall）”吗?
A：若存在上币、做市、自营、投顾等潜在冲突，强烈建议建立信息墙：权限隔离、访问记录、敏感信息分类、违规处罚。

Q255：平台对员工交易有什么要求?
A：建议建立：员工账户申报、预先批准/黑窗期、禁止交易清单、利益冲突申报、抽样监控与纪律处分。

Q256：订单执行质量（Execution Quality）要如何证明?
A：提供：执行政策、滑点统计、成交率、延迟指标、失败原因、客户对账单与争议处理记录。可出具月度执行质量报告模板。

Q257：如何防止“抢跑（front-running）”?
A：关键是系统与治理：

- 订单与市场数据访问分级
- 敏感数据延迟/脱敏策略（按业务）
- 交易监控识别异常
- 员工交易限制与审计
- 违规调查 SOP

Q258：平台是否需要“熔断/限价”机制?
A：强烈建议具备，尤其面向零售。即便不做传统熔断，也应有“异常保护”机制：价格偏离阈值、撮合暂停、订单限制、风控参数自动调整（可解释）。

Q259：平台如何处理“系统故障导致订单未成交/重复成交”?
A：要有纠错与补偿机制：错误识别、回滚/冲正条件（谨慎）、客户通知、补偿原则、监管通报评估、事后复盘与改进。

Q260：平台需要提供 API 吗？API 风险如何控?
A：可以提供，但必须治理：API key 管理、限流、防刷、权限分级、异常行为检测、API 交易监控与日志、终止与封禁机制。

Q261：平台如何处理“高频/机器人交易”?
A：设置：限流、风控参数、反操纵监测、异常撤单率监控、做市商与普通量化策略区分管理。

Q262：平台是否必须做“时间同步与取证”?
A：必须。交易与撮合日志必须具备统一时间源（NTP），且可导出用于监管取证。

Q263：平台的“不可篡改日志”如何实现?
A：可采用 WORM 存储、签名哈希链、权限隔离、审计日志，关键是：能证明日志生成后不可被业务随意修改。

Q264：平台如何满足“记录保存与监管调阅”?
A：建立监管调阅包：订单簿、撮合、取消、转账、费用、对账、告警、投诉、重大事件记录。提供快速检索与导出能力。

Q265：平台是否需要“资产证明/储备证明（PoR）”?
A：MiCA 对客户资产保护与隔离非常重视。PoR 不是唯一方式，但你需要能证明：客户资产隔离、对账、审计、资产迁移与退出可执行。若做 PoR，需说明方法与局限性。

Q266：平台与托管能否分离?
A：可以采用第三方托管或集团内分离，但必须外包治理到位：审计权、数据权、退出权、监管访问权，并证明控制权与客户资产保护仍可实现。

Q267：平台与发行方合作（Launchpad/IEO）有什么风险?
A：冲突与误导营销风险巨大。必须：披露利益关系、风险提示、禁用收益承诺、项目尽调与持续监控、客户适当性与限制。

Q268：如何管理“上币费/推广费”？
A：必须透明：费用性质、用途、与上币决定是否独立、回避机制、内部审批与记录，避免“付费上币”引发操纵与冲突质疑。

Q269：平台是否需要“客户资金与资产隔离账户”？
A：若涉及法币或托管，必须设计隔离账户与对账机制，客户资产不得与自有资产混同。

Q270：平台类业务常见补件点有哪些？
A：Rulebook 不完整、撮合/异常处置不可解释、市场监测缺证据链、上币治理薄弱、冲突管理缺信息墙、日志导出与时间同步不足。

Q271：NBS 面谈对平台类会问什么？
A：通常会问：撮合与公平性、操纵识别与处置、上币/下币机制、冲突管理、客户资产保护、系统安全与日志取证、重大事件处置。

Q272：平台如何处理“跨境客户”与语言披露？
A：即便护照通报，也需做好多语言披露、投诉渠道、营销规则合规补丁，避免落地国消费者保护问题。

Q273：平台能否给客户提供杠杆/衍生品？
A：这通常超出 MiCA 的 CASP 服务边界并可能触发其他金融法规。建议在申请阶段明确“排除项”，避免被认定超范围经营。

Q274：平台对“稳定币交易对”有什么额外关注？
A：关注信息披露、对手方风险、流动性与脱锚风险提示、异常行情预案，以及与发行方关系披露。

Q275：平台如何处理“客户误操作/钓鱼”导致的损失？
A：建立反欺诈机制：2FA、提现白名单、延迟提现、风险提示、客服核验、异常登录检测；并在条款中明确责任边界与可选补偿机制（如适用）。

Q276：平台如何做“黑名单与封禁”？
A：要有政策：触发条件（制裁、诈骗、操纵、AML 高风险）、处置（限制/冻结/关闭）、客户通知策略、申诉与复核、留痕。

Q277：平台需要对做市商进行持续监控吗？
A：必须。监控指标：报价义务履行、异常撤单率、操纵嫌疑、关联交易、对客户执行质量影响。并有处罚与终止机制。

Q278：平台规则变更如何通知客户？
A：要写：变更审批、公告方式、提前通知期、紧急变更例外、客户不同意的退出路径，留存通知证据。

Q279：平台如何处理“链上拥堵导致到账延迟”？
A：披露必须写清：链上确认规则、到账时点、失败/退回处理、费用承担、客服 SLA 与争议处理。

Q280：平台类交付的“验收标准”是什么？
A：监管验收标准：**规则可执行、监测可运行、日志可取证、冲突可解释、客户可保护**。你必须能现场演示并导出证据。

K. 托管（Custody）资产隔离 + 密钥 + 对账 + 责任边界 Q281–Q315

Q281：托管服务最核心的审查点是什么？
A：客户资产保护：**隔离、控制、可证明、可恢复**。监管最怕“你说你托管，但你证明不了你能保护资产”。

Q282：托管架构必须怎么做“隔离”？
A：至少三层隔离：

- **链上地址隔离**（客户分配地址或可追溯子地址）
- **账务隔离**（客户分户账与公司自有账分离）
- **权限隔离**（业务操作与审批/签名分离，最小权限）

Q283：热钱包/冷钱包比例怎么设？
A：应基于风险偏好与运营需求，关键是：热钱包限额、补充规则、异常触发迁移、冷钱包多签/MPC 控制，且留存审批与签名日志。

Q284：HSM、MPC、多签哪个更好？
A：没有“绝对最好”，监管看你能否解释：威胁模型、控制措施、签名门槛、密钥轮换、备份、灾备、演练证据。MPC/多签常见，但必须可审计。

Q285：密钥管理政策必须包含哪些？
A：生成、存储、访问、轮换、备份、销毁、应急恢复、权限审批、签名记录、人员离职权限回收、第三方托管（如有）的审计权。

Q286：托管提现（withdrawal）流程怎么设计最合规？
A：建议“多层控制”：

- 提现白名单/延迟机制（高风险客户）
- 2FA + 设备/行为风控
- 金额阈值触发人工复核
- 多人审批（4-eyes）
- 签名与广播分离
- 交易后对账与异常处置

Q287：如何处理“地址所有权”与自托管提币风险？
A：地址风险评分、可选的所有权证明（签名消息/小额验证）、限额与延迟、异常触发 EDD/拒绝。

Q288：对账（Reconciliation）必须做多频？
A：至少每日；高风险业务建议更高频。对账范围：链上余额、内部账、客户余额、法币隔离账户。差异处理 SOP 必须清晰。

Q289：对账差异怎么处理？
A：建立差异分级：技术延迟/链上拥堵/重复广播/系统错误/内部异常。每类差异有对应处置：暂停、调查、纠错、客户通知、必要时监管通报评估。

Q290：托管是否需要保险（Insurance）？
A：不一定强制，但监管常问。若不投保，要提供替代保障：资本缓冲、风险储备、内部控制、第三方审计、赔付政策与责任边界。

Q291：托管协议（Custody T&Cs）必须披露什么？
A：资产归属、冻结/扣划条件、硬分叉/空投处理、费用、赔付与责任边界、第三方托管披露、争议解决、终止与资产迁移、客户确认留痕。

Q292：如何处理硬分叉/空投的资产归属？
A：必须写清：是否支持、支持条件、分配时间、技术与法律风险、客户通知与争议处理、记录保存。

Q293：如何处理“资产冻结/司法冻结/制裁冻结”？
A：写清权限、审批链、客户通知策略、FIU/监管沟通、解冻条件与记录保存。

Q294：托管资产是否允许再利用（rehypothecation）？
A：如涉及客户资产再利用，会引发极高风险与披露义务，且可能触发更严监管。多数合规交付建议明确“禁止”或严格限制并充分披露与同意机制。

Q295：托管系统需要哪些日志？
A：关键操作日志（创建地址、修改白名单、审批、签名、广播、密钥轮换）、访问日志、异常告警日志、对账日志。要求不可篡改、可导出、时间同步。

Q296：托管外包给第三方可行吗？
A：可行，但外包治理必须非常强：审计权、监管访问权、数据权属、分包限制、退出迁移、事件通报与配合。你仍承担最终责任。

Q297：托管最容易被补件的点是什么？
A：密钥管理写得空、签名流程不可审计、对账不完整、权限隔离不足、外包合同缺审计/退出、赔付与责任边界含糊。

Q298：托管业务的“演示”要演示什么？
A：建议演示：开户→入金→分配地址→转账确认→余额更新→提现审批→签名日志→对账→差异处理案例（模拟）。

Q299：托管如何支持多链/跨链？
A：要写支持范围、跨链风险、桥接策略、无法识别时的限制、日志与对账如何实现。

Q300：如何处理“链上拥堵导致手续费异常/失败”？
A：手续费策略、失败重试规则、客户费用披露、异常工单与客服话术、对账与纠错流程。

Q301：冷钱包灾备怎么做？
A：密钥备份策略、分片存储、地理隔离、恢复演练、恢复审批链、演练记录与整改闭环。

Q302：人员离职/变更对密钥权限影响怎么控？
A：必须有权限回收与密钥轮换触发器：离职即回收、重大岗位变更即轮换、审计记录。

Q303：如何防内部人员作恶？
A：最小权限、双人审批、特权账号审计、行为监控、签名与广播分离、异常阈值触发自动冻结、独立内审抽检。

Q304：如何满足客户资产“可随时交付/可迁移”？
A：要有资产迁移方案：迁移步骤、对账、客户通知、费用、争议处理、第三方托管切换、监管通报策略。

Q305：托管业务与平台撮合能否同系统？
A：可同系统，但必须逻辑隔离：权限与账务隔离、日志隔离、冲突管理与审计路径清晰。

Q306：托管如何处理“误转账/地址错误”？
A：条款与 SOP 要写清：可否找回、找回条件、费用、需要的客户证据、链上不可逆风险提示。

Q307：托管如何处理“代币合约升级/迁移”？
A：要有资产支持政策、升级风险评估、客户通知、测试与演练、对账与争议处理。

Q308：托管如何处理“黑名单地址/受制裁地址”入金？
A：入金识别、冻结/隔离、告警与调查、STR 决策、客户沟通（避免 tipping-off）、记录保存。

Q309：托管服务需要单独的风险储备吗？
A：建议设置风险准备金/运营缓冲（视规模），并在财务模型中体现，用于覆盖安全事件、纠错与客户补偿。

Q310：托管是否必须第三方审计？
A：通常强烈建议：安全审计、财务审计、关键控制审计。即使不强制，监管也会更信任“可验证”的第三方报告。

Q311：托管与 AML/TFR 的关系？
A：托管是 AML/TFR 的高风险触点：出入金、提现到自托管、对手方 CASP 识别、制裁筛查与链上风险评分必须集成。

Q312：托管业务的 KPI/KRI 怎么设？
A：提现审批时效、异常提现率、对账差异率、告警处理时效、热钱包余额占比、权限复核完成率、演练完成率。

Q313：托管业务最关键的“交付包”有哪些?
A：密钥管理政策、签名流程图与审批链、对账 SOP、托管协议与披露包、权限矩阵与日志策略、BCP/DR 与演练记录、外包合同条款包（如适用）。

Q314：托管业务如何应对监管现场抽查?
A：准备：抽样客户钱包地址与余额证明、签名日志、对账记录、权限变更记录、事件演练记录、外包合同与年度评估报告。

Q315：托管模块的验收结论是什么?
A：监管验收结论：**客户资产隔离可证明、密钥控制可审计、对账纠错可执行、外包可控可退出、安全韧性可演练**。

L. 兑换与执行（Exchange / Execution）+ 最佳执行 + 冲突管理 Q316–Q340

Q316：兑换业务（Crypto-Fiat / Crypto-Crypto）最核心的合规点是什么?
A：透明报价、公平执行、费用披露、冲突管理、反操纵与 AML/TFR 联动。

Q317：报价来源（Price Sourcing）需要披露吗?
A：需要。披露：报价来自哪些流动性来源、是否聚合、异常过滤规则、更新频率、对客户的影响（滑点/延迟）。

Q318：价差（spread）与手续费如何披露?
A：必须清晰：价差是否为收入、如何计算、是否会随市场波动变化、客户对账单如何显示；避免“零手续费但加价差”的误导。

Q319：什么是“最佳执行（Best Execution）”在加密里怎么落地?
A：核心是：你要证明执行方式对客户公平且可解释。交付：执行政策、路由规则、滑点统计、失败处理、例外情形与复核机制。

Q320：若平台同时做做市/自营，如何避免客户吃亏?
A：必须：信息隔离、优先权禁止、价格形成披露、独立监控、员工交易限制、定期审计与报告。

Q321：订单传递/代客执行（Execution on behalf）需要什么制度?
A：订单生命周期 SOP、客户指令记录、执行回单、异常与撤销规则、冲突披露、客户投诉路径。

Q322：OTC（场外）属于兑换吗？监管会怎么问?
A：OTC 通常被视为高风险：定价透明度、对手方风险、资金来源、交易监控、录音留痕、报价与确认流程、反欺诈机制。

Q323：OTC 是否必须录音/留痕?
A：强烈建议。至少保留：报价、确认、交易要素、对手方信息、审批链、异常调查记录。

Q324：大额交易如何做风险控制?
A：限额、分级审批、资金来源核验、链上风险评分、TFR 信息完整性校验、必要时延迟或拒绝，并留存证据。

Q325：兑换业务如何处理“价格错误（fat finger/bug）”?
A：必须写纠错机制：错误识别标准、暂停、客户通知、是否回滚/冲正（谨慎）、补偿原则、内部复核与监管通报评估。

Q326：交易失败（failed trade）怎么处理?
A：写清失败原因分类、资金冻结/解冻、重试策略、客户通知、对账与争议处理。

Q327：如何管理“第三方流动性提供者”?
A：准入尽调、合同条款（审计权/事件通报/退出）、报价质量监控、异常处理、冲突披露、年度复核。

Q328：兑换业务需要市场监测吗?
A：建议与平台监测协同，至少要识别对刷、异常价格、关联账户集群、操纵迹象，并能升级到合规/MLRO。

Q329：如何处理“稳定币脱锚”导致客户损失?
A：披露脱锚风险、异常预案（暂停交易/提高风控参数）、客户通知与争议处理、风险评估与复盘。

Q330：客户对账单应展示哪些字段?
A：交易时间、交易对、方向、数量、价格、费用（手续费/价差/第三方费）、成交ID、余额变动、失败/撤销记录。

Q331：如何处理“退款/撤销”?
A：加密交易不可逆，必须披露。若涉及法币退款，要有银行/支付合作流程、反欺诈控制与留痕。

Q332：兑换业务与 AML/TFR 的最强耦合点是什么?
A：出入金、OTC、大额、与自托管互动、与未受监管对手方互动。制度必须把这些场景写成“限制策略+证据链”。

Q333：兑换业务是否需要“风险警示弹窗/冷静期”?
A：面向零售客户强烈建议：高波动资产/高风险场景触发强提示，必要时冷静期与二次确认，留存客户确认。

Q334：如何管理“客户误操作”与欺诈风险?
A：风控：异常登录、设备变更、提现延迟、2FA、电话/视频复核（高风险）、反钓鱼教育与公告、客服 SOP。

Q335：如何证明“执行质量”持续受控?
A：月度执行质量报告：成交率、滑点分布、失败原因、客户投诉关联、异常处置统计；由合规/风控复核并留存。

Q336：兑换与执行模块最常见补件点?
A：报价来源不透明、价差收入不披露、冲突管理薄弱、OTC 留痕不足、执行政策空泛、对账单缺失。

Q337：如果只做“传递订单（RTO)”而不撮合，需要什么重点?
A：重点在：客户指令记录、执行回单、对手方选择与尽调、冲突披露、费用透明、AML/TFR 联动。

Q338：若提供“投顾/组合管理”，兑换执行要加什么?
A：适当性评估、投资指令记录、风险披露增强、利益冲突披露、客户确认与持续监控，外加更严格的合规监督。

Q339：兑换业务是否必须提供“价格偏离解释”?
A：建议提供。尤其当客户质疑成交价时，能用市场数据与报价来源解释，会显著降低投诉与监管风险。

Q340：兑换/执行模块验收结论是什么?
A：监管验收：**报价可解释、费用透明、执行公平、冲突可控、OTC 留痕、对账可核、AML/TFR 可联动**。

M. 信息安全与系统证据链（审批效率决定因素）Q341–Q360

Q341：为什么信息安全会决定审批效率?
A：因为 MiCA 下的 CASP（尤其平台/托管）本质上是“技术驱动的受监管机构”。监管不会只看文字，而会看你是否能证明：权限、日志、事件响应、BCP/DR 都“可运行、可导出”。

Q342：系统架构图需要几张?
A：建议至少三张：

1. 业务流程图（开户→交易→清算→托管→提现）
2. 数据流图（KYC/交易/日志/报表/对外接口）
3. 权限流图（RBAC、特权账号、审批链）

Q343：RBAC 最小权限需要怎么落地?
A：交付：角色表（Role Catalogue)、权限矩阵、特权账号清单、审批流程、季度权限复核记录、离职权限回收记录。

Q344：哪些日志是“监管必看”?
A：KYC 关键操作、订单与撮合、钱包签名与广播、白名单变更、权限变更、风控参数变更、外包接口调用、告警与工单、数据导出操作。

Q345：日志要保存多久?
A：按监管与 AML 记录保存要求设定（通常较长)。关键是：可检索、可导出、不可篡改、访问可审计。

Q346：渗透测试（Pen Test）必须做吗?
A：强烈建议。交付：测试范围、发现漏洞、风险评级、整改计划、复测结论。若外包，也要有供应商报告与你方整改闭环。

Q347：代码审计/合约审计要做吗?
A：若涉及自研撮合、钱包、智能合约或关键组件，强烈建议。监管更信任“第三方可验证”证据。

Q348：事件响应（Incident Response）要包含什么?
A：事件分级、响应角色（含值班)、隔离与止损步骤、取证流程、对内对外沟通模板、监管通报评估、根因分析与整改闭环。

Q349：重大事件的定义如何设?
A：建议结合影响：客户资产、核心服务可用性、数据泄露、制裁/欺诈风险、外包关键故障。并设定触发通报与董事会升级阈值。

Q350：SOC/SIEM 是必须的吗?
A：对平台/托管强烈建议具备。即便规模小，也需具备集中日志、告警、关联分析、留痕与导出能力。

Q351：BCP/DR 的 RTO/RPO 怎么定?
A：应基于业务影响分析（BIA)。关键是：你能解释为何这样定，并能提供演练记录证明可达成。

Q352：灾备演练需要怎样的证据?
A：演练计划、演练脚本、演练结果、问题清单、整改闭环、复测记录。最好包含供应商故障演练。

Q353：如何证明“外包云服务”仍可监管调阅?
A：合同条款 + 技术能力：审计权、监管访问条款、数据导出接口、日志保留、事件通报、退出迁移计划。

Q354：如何管理 API 安全?
A：API key 生命周期、权限分级、限流、防重放、IP 白名单（可选)、异常调用监控、日志与封禁机制。

Q355：如何管理漏洞与补丁?
A：资产清单、漏洞扫描频率、补丁 SLA、例外审批、补丁记录、复核与抽检。

Q356：如何防 DDoS 与基础设施攻击?
A：防护服务、限流、WAF、弹性扩容、应急切换、演练记录与客户通知预案。

Q357：如何做数据备份与恢复?
A：备份频率、加密、访问控制、异地备份、恢复演练、恢复时间指标与记录。

Q358：如何证明“关键参数变更”受控?
A：变更管理（Change Management)：工单、审批、测试、上线窗口、回滚计划、上线后监控、审计记录。

Q359：信息安全培训是否需要?
A：需要。岗位分层（开发/运维/客服/合规)、年度计划、钓鱼演练、考试记录、补训安排。

Q360：信息安全模块最常见补件点？
A：架构与权限不清、日志不可导出、事件响应缺演练、外包条款缺审计/退出、渗透测试缺整改闭环、灾备不可证明。

N. 外包与第三方治理（Outsourcing）+ 供应链风险 Q361–Q375

Q361：什么叫“关键/重大外包（Critical or Important Outsourcing）”？
A：指一旦外包方出问题，会实质影响你持续合规经营、客户资产安全或关键服务可用性的外包。典型包括：

- 云基础设施/托管（IaaS/PaaS）
- 钱包托管/密钥管理（MPC/HSM/多签服务商）
- 核心交易系统/撮合引擎（含 SaaS 平台）
- KYC/身份核验、制裁筛查、链上分析
- Travel Rule 传输通道/消息网络
- 关键客服/工单系统（若影响投诉/留痕）
  关键点：**“是否关键”不以合同金额判断，以“失效影响”判断。**

Q362：外包可以把合规责任也一起外包掉吗？
A：不可以。外包可以做“执行”，但你必须保留：

- 规则/参数与政策所有权（你能改、你能解释）
- 监督与复核能力（你能审计、你能抽检）
- 监管沟通与最终责任（你能问责、你能纠偏）

Q363：外包治理体系至少要交付哪些文件？
A：建议最低“六件套”：

1. Outsourcing Policy（外包政策）
2. Outsourcing Register（外包清单与分级）
3. Third-Party Risk Assessment 模板（尽调评分）
4. Contract Clause Pack（关键条款包）
5. Ongoing Monitoring Plan（持续监测计划/SLA/KPI）
6. Exit Plan（退出与迁移预案）

Q364：外包合同里监管最在意的条款是什么？
A：通常是“五权一案”：

- 审计权（含第三方/内部审计）
- 监管访问权（NBS/相关监管可取证/可调阅）
- 数据权属与可移交（你能导出、能带走）
- 分包限制（分包需批准/透明）
- 事件通报义务（时限、内容、协作）
- 退出迁移方案（Exit Plan）必须可执行

Q365：如果供应商拒绝给“监管访问权/审计权”，怎么办？
A：这是高概率补件甚至卡点。可选路径：

- 更换供应商（最干净）
- 谈判加附录（补上访问/审计/退出条款）
- 使用“审计报告 + 受限审计访问”的替代方案（仍可能被要求强化）
  交付建议：**把关键条款写成“不可谈判红线”。**

Q366：云服务（AWS/Azure/GCP）这种通用云怎么处理审计与退出？
A：做法是“合规组合拳”：

- 合同/条款引用（含标准审计报告、合规证明）
- 你方的“可调阅能力”（日志导出、数据备份、配置基线）
- 退出计划（可迁移架构、数据导出、替代云/本地预案）
- 持续监控（SLA、事件、变更通知订阅、年度复核）

Q367：KYC/制裁筛查/链上分析外包，监管会问什么？
A：常问四点：

1. 模型/命中规则的可解释性（你能解释为何放行/拒绝）
2. 误报/漏报处理（复核、抽检、质量控制）
3. 数据保存与证据链（命中截图、复核记录、审批链）
4. 参数控制权（阈值/规则谁说了算）

Q368：Travel Rule 解决方案外包最容易出问题的点是什么？
A：三点：

- 对接覆盖率不够（对手方不在网络内怎么处理）
- 数据字段不完整/传输失败处理不清晰
- “无法获取信息”的处置（延迟/拒绝/人工复核）没有 SOP 与留痕
  交付建议：把失败场景写成“端到端工单流程”。

Q369：如何做第三方尽调（Due Diligence）才算“可交付”？
A：建议按“五类证据”：

- 资质与合规（公司信息、认证、审计报告、合规声明）
- 安全能力（渗透测试、漏洞管理、访问控制、BCP）
- 财务稳健（持续经营能力、重大诉讼/破产风险）
- 运营与交付（SLA、支持、响应时限）
- 法律与数据（数据驻留、分包、知识产权、退出）
  并输出：评分 + 风险评级 + 缓释措施 + 决策记录。

Q370：供应链风险怎么纳入信息安全体系？
A：把供应商当成“攻击面”。交付：

- 供应商分级（关键/重要/一般）
- 接口与权限最小化（API 权限、密钥轮换）
- 安全事件联动（通报时限、取证协作）
- 年度复核与替代供应商清单（Plan B）

Q371：如果集团内共享服务（IT/合规）算外包吗？
A：通常也要按外包/第三方风险框架治理（“集团内外包”）。监管关心：控制权、审计权、冲突、数据访问与退出。

Q372：外包持续监测要看哪些 KPI/KRI？
A：典型：SLA 达成率、故障次数/时长、事件响应时效、变更通知及时性、数据导出成功率、审计缺陷整改率、支持工单关闭时效。

Q373：外包退出计划（Exit Plan）要写到什么程度？
A：写到“能执行的项目计划”：

- 触发条件（供应商违约/安全事件/监管要求）
- 迁移步骤（数据导出、系统切换、验证）
- 时间表与责任人（RACI）
- 客户通知模板（如影响服务）
- 迁移演练（最好有演练记录）

Q374：外包最常见补件点有哪些？
A：合同缺审计/监管访问/退出条款、外包清单不完整、关键外包未分级、持续监控计划缺失、对供应商“不可控”。

Q375：外包模块的监管验收结论是什么？
A：监管验收看你是否做到：**可控（control）+ 可审（audit）+ 可退（exit）+ 可证（evidence）**。

O. 数据治理 + 记录保存 + 报告导向（含税务/DAC8思路）Q376–Q387

Q376：数据治理为什么会被监管重点关注？
A：MiCA/TFR/AML 与税务报告（如 DAC8 导向）都要求数据“可追溯、可抽取、可解释”。监管检查时，数据就是证据。

Q377：最关键的数据域有哪些？
A：至少四域：

1. 客户数据（KYC/KYB/UBO/风险评级/适当性）
2. 交易数据（订单、成交、费用、对账单）
3. 资产与转账数据（钱包地址、链上Tx、Travel Rule 字段）
4. 合规与运营数据（告警、调查、STR 决策、投诉、事件）

Q378：记录保存通常要保存哪些“证据链”？
A：建议做“可检查目录”：

- 客户开户与审批证据（含 EDD、SoF/SoW）
- 制裁/PEP/负面筛查命中与复核记录
- 交易监控告警→调查→结论→处置全链路
- Travel Rule 传输日志（成功/失败/补救）
- 钱包签名与权限变更日志
- 外包年度评估与审计报告
- 投诉工单与结案证据
- 董事会/委员会决策纪要与附件索引

Q379：如何做到“可抽取的监管报告”？
A：建立“报告数据层”：字段字典、ETL 规则、版本控制、抽样核对、报表生成日志。监管更信任“自动化可重复”。

Q380：数据质量怎么管理？
A：设定数据质量 KPI：完整性、准确性、一致性、及时性；并建立：缺陷工单、根因分析、整改闭环、复核记录。

Q381：如何处理多系统（交易/托管/风控/客服）数据打通？
A：用统一客户ID、统一交易ID、统一时间源；建立主数据（MDM）或数据仓库；确保链上Tx与订单/客户能关联。

Q382：数据留存与隐私/安全怎么平衡？
A：用分级访问控制、脱敏、加密、最小化访问、访问审计；并建立数据请求/导出审批流程。

Q383：如何确保时间戳一致与取证可靠？
A：统一 NTP、日志哈希/签名、不可篡改存储、导出校验。否则监管取证会质疑可信度。

Q384：如果客户要求删除数据怎么办？
A：需在隐私要求与监管保留义务之间平衡：对必须保留的监管数据，通常不能随意删除，应做“限制处理/封存”，并保留法律依据说明。

Q385：数据治理最常见补件点是什么？
A：字段不统一、Travel Rule/链上Tx无法关联到客户、日志不可导出、缺乏数据字典与报表口径说明、数据访问无审计。

Q386：记录保存模块的“交付包”建议有哪些？
A：数据字典、记录保存政策、证据链目录、监管调阅SOP、数据导出审批流程、报表模板与抽取说明。

Q387：数据治理模块监管验收结论是什么？
A：监管验收看：**能不能“从一个客户/一笔交易”追溯到所有证据，并能在短时间内导出。**

P. 投诉处理 + ADR + 争议解决 Q388–Q395

Q388：投诉机制为什么在 MiCA 里是高频问答？
A：因为它直接体现客户保护是否“机制化”。监管不仅看你写了没，还看你能否：按时限处理、留痕、复盘与整改。

Q389：投诉处理流程至少要包含哪些节点？
A：受理→分类分级→分派→调查→回复→结案→复盘→整改闭环。每一步要有时限与负责人。

Q390：投诉分级怎么做？
A：建议三档：

- 严重（涉及资产损失、安全事件、欺诈、重大系统故障）
- 一般（服务质量、延迟、费用争议）
- 建议/咨询
  严重投诉应触发：合规/管理层升级与事件评估。

Q391：ADR（替代性争议解决）要怎么写？
A：写清可用渠道、启动条件、时间线、双方权利义务、证据提交方式、与法院诉讼的关系；并在客户协议与网站披露一致。

Q392：投诉回复要注意什么合规风险?
A：避免泄露敏感信息、避免不当承诺；涉及 AML/制裁/STR 场景要避免 tipping-off；所有沟通要留痕。

Q393：投诉 KPI 要怎么设?
A：受理时效、结案时效、重复投诉率、赔付/纠错金额、根因分类、整改完成率；按月/季度向管理层报告。

Q394：投诉模块最常见补件点?
A：流程没有时限、没有升级路径、没有复盘整改闭环、证据留存不足、客户协议与实际流程不一致。

Q395：投诉/争议模块监管验收结论是什么?
A：监管验收看：**你能否把投诉当成风险信号源，形成闭环治理，而不是客服应付。**

Q. 退出与最后一公里：有序退出/BCP 关联 + 监管补件打法（收尾类）Q396–Q400

Q396：为什么监管会要求“有序退出（Wind-down Plan）”与 BCP/DR?
A：因为 CASP 失败会伤害客户资产与市场信任。监管要看到：即便你出问题，也能“止损、清退、交接、可追责”。

Q397：Wind-down Plan 至少要包含哪些内容?
A：触发条件、客户资产处置、服务停止策略、关键人员替补、外包替换与迁移、客户通知模板、数据封存与监管调阅、时间表与责任人。

Q398：BCP/DR 与 Wind-down 的关系是什么?
A：BCP/DR 是“继续经营情况下的恢复”，Wind-down 是“无法继续经营情况下的有序退出”。两者都要可演练、有证据。

Q399：补件（RFI）应答的黄金结构是什么?
A：每条补件用同一模板：

- 条款依据（MiCA/TFR/AML/本地要求）
- 现状说明（你现在怎么做）
- 改进措施（你将如何补强）
- 证据附件编号（可审计材料）
- 责任人 + 完成日期
- 复核与版本号
  监管最喜欢“闭环”。

Q400：最终交付的“可递交版本”应长什么样?
A：建议输出“ITS 表格 + 附件索引”的提交包：

- 申请表（按 ITS 信息要素）
- 统一 Index（字段→附件页码/段落）
- BdP/CMVM 或 NBS 口径分册（若适用）
- Master Checklist（A–I）对应证据链
- 可演示材料清单（系统、日志、风控、TFR、对账、演练）

仁港永胜建议 + 服务优势 + 联系方式 + 免责声明

仁港永胜建议（可执行清单）

1. **先定服务边界**：把产品拆解到 MiCA 服务类别，形成“服务映射表（产品/流程/条款/制度/系统/证据）”。
2. **先做证据链再递交**：Travel Rule 字段与报文、KYC/EDD 工单、监控告警闭环、权限与日志、钱包签名流程，必须“可演示”。
3. **现金流写实**：把 AML 工具、Travel Rule、SOC/SIEM、审计、渗透测试、外包治理成本写进模型并做压力测试。
4. **外包合同一次到位**：审计权、监管可访问、数据权属、分包限制、事件通报、退出迁移条款缺一不可。
5. **面谈按岗位准备**：管理层/合规/MLRO/IT 安全各自准备“条款—SOP—证据”答题卡。

选择仁港永胜的好处（核心优势）

- **监管导向写作 + Index 交叉引用**：按 ITS/附件编号体系做“可补件、可审计”材料。
- **模板库可直接落地**：AML/Travel Rule SOP、外包条款包、平台规则、上币评估、风控与证据链清单、面谈题库。
- **跨境合规与护照经验**：从 Home Member State 到多国展业的披露/投诉/营销合规补丁可一体化配置。

关于仁港永胜

仁港永胜（香港）有限公司（Rengangyongsheng (Hong Kong) Limited）长期为金融机构、支付机构、加密资产平台、基金与家办提供：

- 牌照申请与持续合规（MiCA CASP、EMI/PI、SFC、MSO、VARA 等）
- AML/CFT 体系搭建、制度与系统合规、监管面谈与检查应对
- 跨境展业合规结构设计（护照机制、集团治理、数据治理）

联系方式

唐上永（唐生，Tang Shangyong）｜业务经理

- 手机 / 微信（深圳）：15920002080
- 香港 / WhatsApp：+852 9298 4213
- 邮箱：Drew@cnjrp.com
- 办公地址：
  - 香港湾仔轩尼诗道 253-261 号依时商业大厦 18 楼
  - 深圳福田卓越世纪中心 1 号楼 11 楼
  - 香港环球贸易广场 86 楼

免责声明

本文由仁港永胜（香港）有限公司拟定，并由唐上永（唐生，Tang Shangyong）提供专业讲解。本文依据欧盟 MiCA / TFR 等公开规则框架与通行监管实践整理，旨在提供一般性合规筹备参考，不构成法律意见、监管承诺或牌照获批保证。具体申请策略、材料清单、审查要点、费用与时间进度应以斯洛伐克主管机关（NBS）及欧盟最新法规、技术标准（RTS/ITS）与个案事实为准。仁港永胜保留对内容更新与修订的权利。

注：本文涉及的模板/清单/电子档（如 Master Checklist、制度模板包、面谈题库等）可向仁港永胜唐生有偿索取。
